Discussing the challenges produced by end-to-end encrypted phones within the mobile forensic aspect of criminal investigations.

Tia C
CMP 416 – Digital Forensics 2

In the last five years, encrypted devices have been showing up within criminal investigations across the world. These encrypted devices allow users to send private messages and content to other device users, without being intercepted. These devices also contain anti-forensic tools, which mean that attempting to gather evidence from these mobile phones is incredibly difficult, most of the time impossible. Previous evidence has been gathered from encrypted devices, through extensive enforcement operations that require hacking and interception. This raises the question of "What challenges are produced by end-to-end encrypted devices and what impact do they have on the mobile forensic aspect of criminal investigations?". This essay will investigate possible methods of evidence acquisition from an encrypted device and whether the presumption of innocence when gathering evidence from an encrypted device is maintained effectively. The essay will also consider the legal challenges faced in using the evidence gathered through hacking and interception and whether it should be admissible within a court of law.

As internet users have become aware of the amount of data and surveillance that is being gathered on them, encryption has become a popular way to protect privacy online. To protect their digital privacy, many people are moving towards encrypted messaging applications such as WhatsApp and Signal. Some users may decide that the app is not suitable for their needs and will opt for an encrypted device to protect their online privacy. End-to-end encrypted devices are mobile phones that have either been created or modified to protect users' communication being intercepted in transmission. It is important to note that possessing and/or using an encrypted device is not illegal, however using encrypted devices for criminal purposes is – which is commonly what they are used for.

EncroChat, Sky ECC, ANOM and EnnetCom are all examples of encrypted devices that were used by criminals and organised crime groups (OCG's). These phones can be described as forensically resistant since they are end-to-end encrypted – the devices also contained extra measures to avoid traceability and evidence acquisition. Some of these measures include removing the camera, microphone, GPS, and USB port; changing the IMEI number each time it is checked; deleting memory on the device when a specific pin was entered or a brute force attempt on the password was made; and messages that were sent to another encrypted device, it could be deleted on that device remotely (Marshall, 2020). This can hamper, as well as potentially cause the termination of an investigation due to lack of suitable evidence.

Mobile forensics is a sub-category of digital forensics and is considered as the "*science of recovering potential digital evidence from mobile devices using similar techniques as for digital forensic investigations"* (Mumba et al, 2014). Mobile forensics focuses primarily on the forensics of mobile devices such as mobile phones and tablets. As mobile devices are becoming much more accessible and are used more regularly than other digital devices, evidence is accumulated at a larger volume. As well as this, mobile devices are constantly being updated and changed, which means that the way evidence is acquired needs to be updated and changed to reflect this too.

The '*ACPO Good Practice Guide for Computer-Based Electronic Evidence*' is referred to by digital forensic practioners throughout an investigation within the UK. These guidelines are used to ensure that digital evidence is gathered in a forensically and legally sound manner, as to ensure the admissibility of evidence in court (ACPO, 2012). These guidelines have four principles that should be adhered to within an investigation; the first being, that evidence stored on a computer or storage device, should not be changed by law enforcement. The second is that if a copy of best evidence cannot be created and the original must be used for evidence acquisition, the person must be certified and able to be a witness within the court to explain their actions. The third is that an audit trail should be present and that third parties are able to carry out the same procedure and get the same result, whilst the fourth is that the person leading the investigation ensures the principles and law are upheld throughout the investigation.

However, with encrypted devices this encrypted devices such as EncroChat and SkyECC containing anti-forensic measures, this causes challenges within mobile forensic investigations. Attempting to adhere to the ACPO guidelines may not be feasible or entirely possible due to these measures. For example, principle one of the ACPO guidelines which is to ensure data is not changed may not be possible, as trying to copy the device's contents could cause the device to wipe itself meaning any potential evidence would be lost. As well as this, if a practioner attempted to brute force the PIN or enter an incorrect PIN given by the suspect, it could potentially trigger a panic switch/kill switch which would wipe the device. Principle two may also not be feasible due to the likelihood of being able to access the device in an unlocked state. The device may be in an unlocked state when first responders and/or a law enforcement team have made their way into a property where the suspect is actively using the device. If the device is in an unlocked state, an on-site triage can take place where evidence may be gathered from the device – however, the individual may not be competent with mobile forensics or the device itself, leading to an ineffective triage. This could possibly lead to the device locking itself, wiping itself or the opportunity for evidence acquisition to be missed.

The ACPO guidelines also detail how devices that may contain evidence should be gathered and stored upon searching an area, as well as how evidence should be acquired from these devices. This again ensures that evidence is acquired in such a way that it is not altered and is admissible in a court of law, to support the accusations against the suspect. Encrypted devices can cause challenges to these guidelines due to the anti-forensic tools and methods installed in the device. Mobile identification can be difficult, due to the devices using popular phones such as iPhones and Google Pixels as 'shells' to house the device itself and the IMEI number changes regularly within the device. If the device is locked, the data will be encrypted regardless of the device being in 'After First Unlock' or 'Before First Unlock' – meaning even if the device is accessed through forensic tooling, the data will still be in an encrypted state. On-site triaging may also not be entirely feasible if the suspect has alerted other users to a police presence, as they can remotely delete messages and evidence from the device. However, placing an unlocked device in the faraday bag or box, can also cause the device to time-out and lock itself preventing any evidence acquisition or the battery may be drained as the devices attempts to reconnect to the network.

The ACPO guidelines do not address the challenges that anti-forensic methods and tools may have on an investigation and court proceedings. The paper '*Digital Forensics vs. Anti-Digital Forensics: Techniques, Limitations and Recommendations.'* discusses the impact that anti-forensics techniques can have on mobile forensic investigations. It does not discuss encrypted mobile devices directly but does go into detail about the various anti-forensic methods that can affect investigations. The paper discusses incompatibility, data wiping, data hiding, data location and cryptographic challenges as limitations in mobile forensics investigations, which encrypted devices employ as anti-forensic methods (A. Yaacoub et.al, 2021).

Incompatibility pertains to the forensic tools that are used by cyber crime units to process and examine devices for evidence acquisition. Encrypted devices will be unknown to these tools and as such, will be incompatible with the tools and software being used for the investigation. Data wiping is when either the user or the device itself wipes the storage to avoid data being used as evidence – encrypted devices employ this through remote and manual means. Data location refers to the data being stored either locally on the device or remotely on a secure server, this can cause issues as the evidence that is required may not be accessible through forensic means. Some encrypted devices may store all the data on the phone directly and encrypt it, whilst some may require the device to connect to the server and access the data that way, which means that the data will not be accessible to the practitioner. Cryptographic challenges relate to the issue that encryption has on investigations and evidence acquisition and the inability to use encrypted evidence as there is no way to decrypt it for analysis. This demonstrates that encrypted devices may not be suitable for evidence acquisition due to the inability to physically crack the encryption on the device and data.

These papers highlight the issue that mobile forensic techniques are not currently suitable for gathering evidence from encrypted mobile devices. These methods are likely to cause greater disruption in other investigations that are not surrounding encrypted devices, which further highlights the need for mobile forensic techniques to become more advanced and up to date. However, law enforcement agencies across the world have taken a more direct approach to encrypted devices being used by OGCs, through the means of interception and hacking.

With OCGs across the world using encrypted devices to communicate with each other, it has become a large target for law enforcement agencies across the world. In 2017, when carrying out criminal investigations and operations, French law enforcement discovered that EncroChat phones were being used within OCGs for criminal operations. This led to French and Dutch law enforcement coming together to form a Joint Investigation Team (JIT) through Europol, which is the European Union Agency for Law Enforcement Cooperation.

On the 13th of June 2020, EncroChat sent a message out to all users stating that the servers had been seized and that the platform had been intercepted. According to Marshall (2020), the JIT had exploited a vulnerability within the server, allowing law enforcement to upload their own version of the operating system to user's EncroChat devices. This allowed the JIT and Europol to intercept the communication between the criminal groups and begin collecting evidence. This information was gathered between April 2020 to the 13th of June when EncroChat sent the warning to users. The evidence that was gathered was reviewed and shared with countries that were affected by OCG that were using EncroChat devices such as the UK, Norway, and Sweden. Within two weeks of the message being sent, the National Crime Agency *(NCA. 2021)* in the UK reported that they had "…punched huge holes in the UK organised crime network so far by arresting 746 suspects and seizing over £54 million in criminal cash, 77 firearms… more than two tonnes of Class A and B drugs…". The NCA has also claimed that the EncroChat information provided by Europol allowed for the "biggest and most significant operation of its kind in the UK".

After the shutdown of EncroChat, many of the criminal groups were left with no way to communicate and thus had to find a new encrypted communication device. Sky ECC was a competitor in the encrypted device market, when EncroChat was taken down – many users moved onto other providers, with many choosing Sky ECC. Europol stating that there were "approximately 170,000 individuals… around three million messages exchanged each day" using Sky ECC before it was taken down. Law enforcement agencies within Belgium, France and the Netherlands were able to break the encryption and gain the 'key' for all the encrypted messages within the Sky ECC servers. Within these 170,000 individuals - 70,000 of these individual's conversations were monitored by law enforcement – leading to "a large number of arrests… numerous house searches and seizures in Belguim and the Netherlands". Two months later, the Sky ECC evidence was used in an operation that disrupted the 'Ndrangheta mafia in Italy; 35 suspects were arrested, and 65 others were identified.

When Sky ECC was taken down – criminal gangs once again had to find a new private communication method; many opted for ANOM – which was specifically aimed at criminals. The devices were endorsed by key criminals in the organised crime network, which then encouraged more criminals to use the ANOM app and device. However, ANOM was a honeypot operated by the FBI and Australian law enforcement. As ANOM was being run by law enforcement, there was no need for any hacking of devices or interception of messages. According to the BBC, at least 800 criminals were arrested across the world and Australian Law enforcement said that "Operation Ironside was a watershed moment in Australian law enforcement history" which led to 224 suspects being arrested, three tonnes of drugs and £25 million in cash assets being seized and had identified and disrupted 20 threats of murder (Kleinman, Z, 2021).

However, it can be argued that the evidence gathered from these operations was not gathered in a manner that would not typically be admissible in a court of law. This could potentially mean that the suspects who were arrested, may not be charged with the crime they are accused of due to lack of admissible evidence. The ACPO principles were not adhered to as there is no accessible information stating that data was not changed law enforcement, there is no information on the operation and how the interception taken place, there is no audit trail from the law enforcement and the commander was not able to ensure the principles were adhered to (UK courts face evidence 'black hole' over police

EncroChat mass hacking, 2021). This has been considered within a court of appeal hearing and many expert witnesses within digital forensics have said that the evidence is not reliable and “lacks corroborating evidence”.

As well as this, the presumption of innocence was also a factor that was affected by the EncroChat operations. Presumption of Innocence is part of the Human Rights Act, within the ‘Right to a fair trial’ that “Everyone charged with a criminal offence shall be presumed innocent until proven guilty according to law” (Human Rights Act 1998, 2000). The paper ‘Digital evidence: Unaddressed threats to fairness and the presumption of innocence’ discusses how the interception of the EncroChat messages interfered with suspect’s rights to privacy and data protection (Stoykova, 2021). The paper emphasises that “90% of criminal investigations nowadays have a digital element” and that the methodology and tools used within digital forensic investigations are not validated effectively. Stoykova also directly refers to the EncroChat evidence and that the audit trail is essentially hidden as military secrets, which means that the reliability of the evidence cannot be determined. The interception of EncroChat was carried out by French law enforcement, who have different laws to the UK, which means that actions considered unlawful by the UK may be lawful under French law – which raises questions about the admissibility of the evidence and if it is reliable to be used in a court of law in a criminal case.

Rather than using hacking and interception to gather evidence that may not be admissible in a court of law, mobile forensics should be the preferred method. However, to acquire digital evidence from encrypted devices in both a forensically and legally sound manner, mobile forensics techniques and guidelines will need to adapt to overcome these challenges.

A paper written by Fukami et al, introduces ‘A new model for data extraction from encrypted mobile devices’. The paper acknowledges that current mobile forensic techniques and frameworks are not up to date, and that more invasive techniques and tools are required. As more devices employ encryption to protect user’s privacy, the greater the challenge of accessing digital evidence on these devices – this leads to forensic practioners using more invasive tools and techniques to access the device. The paper also discusses the implications of encryption through manual and logical extractions, in that the data will still require decryption regardless of the extraction technique used if a password or decryption key is not available. To bypass these challenges, the authors recommend that a new framework that regulates the use of invasive techniques for forensic purposes is created, with an emphasis of the use of reverse engineering and vulnerability exploitation to be used on seized devices (Fukami et al, 2021).

The framework that Fukami et al presents, would ensure that suspects’ Presumption of Innocence and human rights are not being violated. The framework would also allow for the APCO guidelines to be followed precisely by ensuring that data is not changed and that there is an audit trail, compared to the EncroChat data. The framework would not only benefit investigations of encrypted devices such as EncroChat and Sky ECC but would also apply to devices such as iOS and android phones that use file and disk-based encryptions.

With law enforcement taking encrypted communication services down, there is the possibility that the encryption may get stronger, or the OCGs will simply stop using encrypted devices. The paper ‘The fall of EncroChat and the future of Criminal Communications’ introduces the possibility that encrypted devices will continue to be used by OCGs for criminal communications. Marshall also discusses the possibility that rather than relying on encryption and being secretive, criminals may move to steganography and posting in plain sight. The paper emphasises the fact that encrypted communications will continue to be used, but that encrypted apps may also be used instead, to prevent suspicions being raised over the possession and use of an encrypted device (Marshall, 2020). This further emphasises the need for a new mobile forensics framework to be developed, so that these issues can be tackled before they become major challenges in investigations.

A conference paper by Pisaric titled, ‘Encrypted Mobile Phones’ details the encrypted phones that have been taken down by law enforcement, but also discusses the possible future and outcome of these actions. The paper shows that OCGs simply move onto the next encrypted device provider when the current provider they are using is shut down, which is also demonstrated in the ‘Fall of Encrochat paper’, where Marshall explains that users will continue to use encrypted devices. Pisaric also discusses the legality and admissibility of the evidence that has been obtained as a reason why OCG may continue to use encrypted devices (Pisaric M, 2021). This paper demonstrates the need for mobile forensics to be updated, so that evidence gathered from encrypted devices can be used as admissible evidence – which may likely prevent OCGs from using these communication devices as they would not be as private and secure as once thought.

In conclusion, end-to-end encrypted devices can cause a multitude of challenges for mobile forensic investigations. These challenges can vary from; incompatibility of the devices with forensic tools, anti-forensics tools within the encrypted devices such as data wiping and data encryption, and the inability to acquire evidence from memory and storage. There are also challenges caused by the evidence gathered through interception and hacking by law enforcement, particularly pertaining to the legality of the evidence.

Encrypted devices are likely going to be continued to be used by OCG’s as their main communication device between each other for criminal purposes. The encrypted devices are only going to be created with stronger encryption and possibly use steganographic abilities too, which means that mobile forensics will need to change and update to consider these challenges. To be able to mitigate these challenges, a new framework needs to be created, as well as practioners being competent in new techniques such as reverse engineering and vulnerability exploitation.

References

7safe.com. 2021. *ACPO Guidelines | Publications | 7Safe*. [online] Available at: <https://www.7safe.com/trainingoverview/acpo-guidelines> [Accessed 29 November 2021].

ComputerWeekly.com. 2021. *UK courts face evidence 'black hole' over police EncroChat mass hacking*. [online] Available at: <https://www.computerweekly.com/news/252498544/UK-courts-face-evidence-black-hole-over-police-EncroChat-mass-hacking> [Accessed 29 November 2021].

Europol. 2021. *Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe*. [online] Available at: <https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe> [Accessed 23 November 2021].

Europol. 2021. *New action at EU level against 'Ndrangheta in Italy and Germany*. [online] Available at: <https://www.europol.europa.eu/newsroom/news/new-action-eu-level-against-%E2%80%98ndrangheta-in-italy-and-germany> [Accessed 28 November 2021].

Fukami, A., Stoykova, R. and Geradts, Z., 2021. A new model for forensic data extraction from encrypted mobile devices. *Forensic Science International: Digital Investigation*, 38, p.301169.

Judiciary.uk. 2021. *A, B, D & C -v- Regina*. [online] Available at: <https://www.judiciary.uk/judgments/a-b-d-c-v-regina/> [Accessed 19 November 2021].

Kleinman, Z., 2021. *ANOM: Hundreds arrested in massive global crime sting using messaging app*. [online] BBC News. Available at: <https://www.bbc.co.uk/news/world-57394831> [Accessed 20 November 2021].

Legislation.gov.uk. 2021. *Human Rights Act 1998*. [online] Available at: <http://www.legislation.gov.uk/ukpga/1998/42/schedule/1 /part/I/chapter/5> [Accessed 29 November 2021].

Marshall, Angus. (2020). The fall of EncroChat and the future for criminal communications.

Mumba, E. and Venter, H., 2014. Mobile forensics using the harmonised digital forensic investigation process. *2014 Information Security for South Africa*,.

NCA. 2021. *NCA and police smash thousands of criminal conspiracies after infiltration of encrypted communication platform in UK's biggest ever law enforcement operation*. [online] Available at: <https://nationalcrimeagency.gov.uk/news/operation-venetic> [Accessed 23 November 2021].

Pisaric, M., 2021. *ENCRYPTED MOBILE PHONES*. [online] Eskup.kpu.edu.rs. Available at: <http://eskup.kpu.edu.rs/dar/article/view/293> [Accessed 29 November 2021].

Stoykova, R., 2021. Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review*, 42, p.105575.

Yaacoub, Jean-Paul & Noura, Hassan & Salman, Ola & Chehab, Ali. (2021). *Digital Forensics vs. Anti-Digital Forensics: Techniques, Limitations and Recommendations.*